DoD Bluetooth Smart Card Reader Security Requirements Matrix

Version 2.0

June 1, 2007

This matrix was developed by the DISA Field Security Operations (FSO) and is an unofficial compilation of DoD security requirements for DoD Bluetooth Smart Card Readers (SCR). The purpose of the matrix is to provide a tool for DISA FSO when evaluating Bluetooth SCRs. The requirements listed in this document are subject to change as new security vulnerabilities are identified or DoD commands or agencies provide comments to DISA.

A copy of this matrix will be provided to DoD commands/agencies and vendors upon request (send an email request to http://fso_spt@disa.mil).

See Requirement 25.0 in the **DoD Wireless Push Email System Security Requirements Matrix**, version 2.0, 1 June 2007, for information on handheld device security Bluetooth requirements.

Changes from previous version:

-Previous version was 1.0, dated Oct 27, 2006.

-Requirement 2.0. Reorganized and added new information (Requirement 2.3).

Requirement Number	Requirement	Source of Requirement
1.0	Bluetooth mutual authentication, 128 bit Bluetooth encryption, and FIPS 140-2 certified cryptography must all be used for all communications between the smart card reader and the host device.	NSA Bluetooth Security Team
2.0	Bluetooth Pairing requirements	NSA Bluetooth Security Team
2.1	Bluetooth pairing passkeys must be at least eight decimal digits in length and generated randomly.	
2.2	Pairing should be done as infrequently as possible, ideally in a secure area where attackers cannot realistically observe the passkey entry and intercept Bluetooth pairing messages. (Note: A “secure area” is defined as a non-public area that is indoors away from windows in locations with physical access controls.)	
2.3	Bluetooth mutual authentication immediately after the initial establishment of any Bluetooth connection	
3.0	The Bluetooth smart card reader must remain undiscoverable to other Bluetooth devices at all times other than the initial pairing process and cannot initiate Bluetooth connections on its own. It should only support the minimal amount of Bluetooth services required for use as a smart card reader for a single host device.	NSA Bluetooth Security Team
3.1	Unnecessary Bluetooth services, user controls, and applications must be either removed from the host device or reliably disabled permanently.	NSA Bluetooth Security Team
3.2	All Bluetooth profiles except for Serial Port Profile shall be disabled at all times. User cannot enable.	NSA Bluetooth Security Team